



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

Censoring Representations with an Adversary

Citation for published version:

Edwards, H & Storkey, A 2016, Censoring Representations with an Adversary. in *International Conference in Learning Representations (ICLR2016)*. pp. 1-14, 4th International Conference on Learning Representations, San Juan, Puerto Rico, 2/05/16. <<https://openreview.net/forum?id=ByuP8yZRb>>

Link:

[Link to publication record in Edinburgh Research Explorer](#)

Document Version:

Peer reviewed version

Published In:

International Conference in Learning Representations (ICLR2016)

General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



CENSORING REPRESENTATIONS WITH AN ADVERSARY

Harrison Edwards & Amos Storkey

Department of Informatics

University of Edinburgh

Edinburgh, UK, EH8 9AB

H.L.Edwards@sms.ed.ac.uk, A.Storkey@ed.ac.uk

ABSTRACT

In practice, there are often explicit constraints on what representations or decisions are acceptable in an application of machine learning. For example it may be a legal requirement that a decision must not favour a particular group. Alternatively it can be that that representation of data must not have identifying information. We address these two related issues by learning flexible representations that minimize the capability of an adversarial critic. This adversary is trying to predict the relevant sensitive variable from the representation, and so minimizing the performance of the adversary ensures there is little or no information in the representation about the sensitive variable. We demonstrate this adversarial approach on two problems: making decisions free from discrimination and removing private information from images. We formulate the adversarial model as a minimax problem, and optimize that minimax objective using a stochastic gradient alternate min-max optimizer. We demonstrate the ability to provide discriminant free representations for standard test problems, and compare with previous state of the art methods for fairness, showing statistically significant improvement across most cases. The flexibility of this method is shown via a novel problem: removing annotations from images, from separate training examples of annotated and unannotated images, and with no a priori knowledge of the form of annotation provided to the model.

1 INTRODUCTION

When we apply machine learning techniques many real-world settings, it is not long before we run into the problem of sensitive information. It may be that we want to provide information to a third party, but be sure that third party cannot determine critical sensitive variables. Alternatively it may be that we need to make decisions that do not treat one category differently from another. Two specific cases of this are image anonymization and fairness respectively.

1.1 FAIRNESS

As more of life’s decisions become automated there is a growing need, for legal and ethical reasons, to have machine learning algorithms that can make *fair* decisions. A decision is fair if it does not depend upon a sensitive variable such as gender, age or race. One naive approach to achieving a fair decision would be to simply remove the sensitive covariate from the model. But information about the sensitive variable can ‘leak’ back into the decisions made if there is any dependence between it and the other variables. In this work we focus on *fair classifiers* where we want to predict a binary variable Y and be fair with respect to a binary sensitive variable S . Here, fairness means that the decision is not-dependent on (i.e. marginally independent of) the sensitive variable.

Previous works, such as those listed in Section 2.2, have tended to develop specific fair variants of common classifiers to solve this problem. Our approach, called *adversarial learned fair representations* (ALFR), is to learn representations of the data which are concurrently both fair and discriminative for the prediction task. These features can then be used with any classifier. To achieve both fair and discriminative properties, we represent this as a dual objective optimization problem that can be cast as a minimax problem. We maintain the flexibility of both the representation and the

test of fairness, by using deep feed-forward neural networks for each part. There is a deep neural network that is used to produce the representation; that representation is then critiqued by a deep neural adversary who tries to predict the sensitive variable from the representation.

In this paper, we introduced the adversarial method ALFR as a minimax problem, describe the optimization process, and evaluate ALFR on two datasets, *Diabetes* and *Adult*. This demonstrates improvement over a related approach Zemel et al. (2013). We also, as an aside, provide the relationship between the discrimination of a classifier and the H-divergence, as used in domain adaptation. The relationship of these methods to domain adaptation is interesting: the different cases for the sensitive variable can be thought of as different domains. However, we leave the study of this for another paper.

1.2 IMAGE ANONYMIZATION

There are many notions and problems relating to privacy in the literature. Strict forms of privacy such as that enforced by differential privacy are not always necessary, and more relaxed notions of privacy are beneficial in reducing distortion and making more accurate analysis possible. One particular case of privacy is where certain parts of the data should not be communicated (e.g. someones address or name). However in many settings it is hard to be explicit about exactly what should not be communicated or whether that information is coupled with other measured variables.

In this work we consider the concrete case of removing private information from an image, whilst distorting the image as little as possible. Examples of private information include: licence plates on cars in photos and doctors' annotations on medical images such as X-rays. We suggest a modification of an autoencoder to remove such private information, and validate this idea by removing surnames from a collection of images of faces. A similar application might be removing logos or watermarks from images.

The novelty of our approach is that the model does not need to be trained with aligned input/output examples, rather only examples of inputs and (separately) examples of outputs, labelled as such. For example if the task is to remove text from an image, an aligned input/output pair would be an image containing text, and the same image with the text removed. Unaligned data would simply be images labelled as containing no text, and images labelled as containing text. The former sort of data would often be substantially more difficult to obtain than the latter.

Once again we use the same two-neural-network minimax formalism to characterise the problem, and the same stochastic gradient optimization procedure to learn the neural network parameters. The model is applied to the problem of images with and without annotation, to good visual affect. A neural network can no longer distinguish well between annotated and non-annotated images, and the actually annotation itself is obscured.

2 RELATED WORK

2.1 ADVERSARIAL LEARNING

The idea of adversarial learning is that one has a representation R , a dependent variable S and an adversary that tries to predict S from R . The adversary then provides an adaptive measure of dependence between R and S which can then be used to learn R so that it minimizes this dependence.

The adversarial approach was, to the best of our knowledge, introduced in Schmidhuber (1991) where it was used to learn a representation of data $R = (R_1, \dots, R_d)$ where each R_i is both binary and independent of the other R_j . The experiments in this work were on synthetic data, and were later followed up to learn filters from natural image patches in Schmidhuber et al. (1996) and Schraudolph et al. (1999). They referred to this approach as the *principle of predictability minimization*.

More recently in Goodfellow et al. (2014) the idea of using an adversary to learn a generative model of data was introduced and followed-up by work such as Gauthier (2015), Rudy & Taylor (2014) and Denton et al. (2015). In this setting the representation R is a mixture of data samples and generated samples, and S is a binary variable indicating whether a given sample is from the data or 'fake'. For discussion on using 'distinguishability criteria' to learn generative models see Goodfellow (2014).

The inspiration for ALFR comes from using adversarial learning to do domain-adaptation in Ganin et al. (2015). In this setting S is a variable indicating the domain, and the idea is to learn a representation R in which the domains are indistinguishable, motivated by bounds in Ben-David et al. (2010) relating performance on the target domain (the new domain to which we want to adapt) to the dissimilarity of the target and source domains.

2.2 FAIR CLASSIFIERS

Several works have proposed variants of classifiers that enforce fairness. These include discrimination-free naive-Bayes (Calders & Verwer (2010)), a regularized version of logistic regression (Kamishima et al. (2011)), and a more recent approach Zafar et al. (2015), where the authors introduce constraints into the objective functions of logistic regression, hinge-loss classifiers and support vector machines.

Another approach is *data massaging*, whereby the labels of the training data are changed so that the training data is fair (Kamiran & Calders (2009)), this is similar to the resampling methods often used to tackle class-imbalance problems.

An approach more in the spirit of ALFR is *learned fair representations* (LFR) (Zemel et al. (2013)). In that paper, the authors learn a representation of the data that is a probability distribution over clusters — a form of ‘fair clustering’ — where learning the cluster of a datapoint tells one nothing about the sensitive variable S . The clustering is learned to be fair and also discriminative for the prediction task.

Other than LFR, the previous work has focused on enforcing fair decisions, whereas LFR and ALFR aim to get fairness as a side-effect of fair representations. The advantage of the latter approach is that the representations can potentially be reused for different tasks, and there is the possibility of a separation of concerns whereby one party is responsible for making the representations fair, and another party is responsible for making the best predictive model. In contrast to LFR, our approach is more flexible in terms of the kinds of representations it can learn, whereas LFR learns essentially categorical representations. In addition our approach means that the representations can be used with any classifier.

Concurrent with this work is the preprint ‘The Variational Fair Autoencoder’ (Louizos et al. (2015)). There are two main differences between this work and theirs. First they use a variational autoencoder that factorizes the latent variables Z and sensitive variable S . This aspect is complementary and could be incorporated into the adversarial framework. Secondly they use a Maximum Mean Discrepancy (MMD) penalty to reduce dependence of the representation on S , this is a kernel-based alternative to using an adversary. It is not yet clear in what circumstances we should prefer MMD over an adversary, we hope that future work will address this question.

2.3 REMOVING PRIVATE INFORMATION

The problem of removing information from images in a learned manner has not been tackled, to the best of our knowledge, in the machine learning community. However there has been work on detecting when private information has been erroneously left in an image, such as in Korayem et al. (2014) and Erickson et al.

3 FORMALISM: FAIRNESS AND DISCRIMINATION

We consider a binary classification task where $\mathcal{X} \subset \mathbb{R}^n$ is the input space, $\mathcal{Y} = \{0, 1\}$ is the label set and $\mathcal{S} = \{0, 1\}$ is a protected variable label set. We are provided with *i.i.d* examples $\{(x_i, y_i, s_i)\}_{i=1}^m$ drawn from some joint distribution P over corresponding random variables (X, Y, S) . The goal of the learning algorithm is to build a classifier $\eta : \mathcal{X} \rightarrow \mathcal{Y}$ that has high accuracy whilst maintaining the property of *statistical parity* or *fairness*, that is

$$P(\eta(X) = 1 | S = 1) = P(\eta(X) = 1 | S = 0). \quad (1)$$

A key statistic we will use to measure statistical parity is the *discrimination* defined

$$y_{disc} = \left| \frac{\sum_{i:s_i=0} \eta(x_i)}{N_0} - \frac{\sum_{i:s_i=1} \eta(x_i)}{N_1} \right|, \quad (2)$$

where N_0, N_1 are the number of data items where s_i equal to 0 and 1, respectively. We measure the success of our classifier using the empirical accuracy y_{acc} .

Following Zemel et al. (2013) we aim to optimize the difference between discrimination and classification accuracy

$$y_{t,delta} = y_{acc} - t \cdot y_{disc}, \quad (3)$$

where $t \geq 0$, called the *delta*. In Zemel et al. (2013) they consider the specific trade off where $t = 1$, whereas we will evaluate our models across a range of different values for t .

4 CENSORED REPRESENTATIONS

In this section we show how a modification of an autoencoder can be used to learn a representation that obscures/removes a sensitive variable. In the general case we have an input variable X , a target variable Y and a binary sensitive variable S . The objective is to learn a representation $R = \text{Enc}(X)$ that preserves information about X , is useful for predicting Y and is approximately independent of S . The loss we will use is of the form

$$L = \alpha C(X, R) + \beta D(S, R) + \gamma E(Y, R) \quad (4)$$

where C is the cost of reconstructing X from R , D is a measure of dependence between R and S and E is the error in predicting Y from R . The scalars $\alpha, \beta, \gamma \geq 0$ are hyperparameters controlling the weighting of the competing objectives. If we don't have a specific prediction task, as in the case where we just want to remove private information from an image, then we don't need the γ term. On the other hand, if we are not interested in reusing the representation for different predictive tasks then we may set $\alpha = 0$. We may also want to have $\alpha > 0$ in the case where we want to learn a transformation of the data $X \rightarrow \hat{X}$ that is fair and preserves the semantics of the representation, for example in certain regulated areas the interpretability of the model is paramount. Notice also that only the final term depends-upon Y and so there is an opportunity to train in a semi-supervised fashion if the labels are not available for all of the data.

4.1 QUANTIFYING DEPENDENCE

We begin with quantifying the dependence $D(S, R)$ between the representation R and the sensitive variable S . Since S is binary, we can think of this as measuring the difference between two conditional distributions: $R_0 \sim R|S=0$ and $R_1 \sim R|S=1$. We will do this by training a classifier to tell them apart, called the *adversary*. Interested readers may wish to know that this measure of dependence is related to the notion of an \mathcal{H} -divergence, as described in Appendix A.

In particular if the adversary network $\text{Adv} : \mathcal{R} \rightarrow [0, 1]$ trained to discriminate between R_0 and R_1 has parameters ϕ , and the encoder $\text{Enc} : \mathcal{X} \rightarrow \mathcal{R}$ has parameters θ , then we can define

$$D_{\theta, \phi}(R, S) = \mathbb{E}_{X, S} S \cdot \log(\text{Adv}(R)) + (1 - S) \cdot \log(1 - \text{Adv}(R)), \quad (5)$$

that is the *negative* of the standard log-loss for a binary classifier. The adversary's parameters ϕ should be chosen to maximize D (and hence to approximately realize the empirical \mathcal{H} -divergence $\hat{d}_{\mathcal{H}}(A, B)$), whilst the representation parameters θ should be chosen to minimize D (and hence to approximately minimize $\hat{d}_{\mathcal{H}}(A, B)$), so we have a minimax problem:

$$\min_{\theta} \max_{\phi} D_{\theta, \phi}(R, S). \quad (6)$$

Of course, this admits a trivial solution by learning a constant representation R , and so we must introduce constraints to learn anything interesting.

4.2 QUANTIFYING $C(X, R)$

We quantify the information retained in R about X by the ability of a decoder $\text{Dec} : \mathcal{R} \rightarrow \mathcal{X}$ to reconstruct X from R , in particular we use the expected squared error

$$C_\theta(X, R) = \mathbb{E}_X \|X - \text{Dec}(R)\|_2^2, \quad (7)$$

where we extend θ to include the parameters in the decoder Dec .

4.3 QUANTIFYING $E(Y, R)$

We quantify how discriminative R is for the prediction task using the log-loss of a classifier or predictor network $\text{Pred} : \mathcal{R} \rightarrow [0, 1]$, trained to predict Y from R :

$$E_\theta(R, S) = - \mathbb{E}_{X, Y} Y \cdot \log(\text{Pred}(R)) + (1 - Y) \cdot \log(1 - \text{Pred}(R)), \quad (8)$$

where we again extend θ to encompass the parameters of the predictor network Pred .

4.4 OPTIMIZATION

There are four elements in the model: the encoder, the decoder, the predictor and the adversary. Each is implemented using a feed-forward neural network, the precise architectures are detailed in Section 5. The costs for these elements, given in equations 8, 5 and 7, are joined together to give the joint loss

$$L(\theta, \phi) = \alpha C_\theta(X, R) + \beta D_{\theta, \phi}(R, S) + \gamma E_\theta(Y, R) \quad (9)$$

This enables the problem of learning censored representation to be cast as the minimax problem

$$\min_{\theta} \max_{\phi} L(\theta, \phi). \quad (10)$$

Expecting to be able to train the adversary in the inner loop to a global optimum is unrealistic. Instead, as described in Goodfellow et al. (2014) we use a heuristic: a variant on stochastic gradient descent where for each minibatch we decide whether to take a gradient step with respect to the actors parameters θ or a negative gradient step with respect to the adversary’s parameters ϕ . In Goodfellow et al. (2014) they consider simple strict alternation between updating the adversary and actor, we find this to be a useful default. We give detailed pseudo-code for strict alternation in Algorithm 1. Note that the gradient steps in Algorithm 1 can easily be replaced with a more powerful optimizer such as the *Adam* algorithm (Kingma & Ba (2014)). This method is a heuristic in the sense that we do not provide formal guarantees of convergence, but we do know that the solution to the minimax problem is a fixed point of the process. There are a large number of papers using this method (such as those mentioned in 2.1) and getting good results, so there is considerable empirical evidence in its favour.

The key issue in this process is that if the adversary is too competent then the gradients will be weak for the actor, whereas if the adversary is too incompetent then the gradients will be uninformative for the actor. We have also considered not updating the adversary if, for instance, its accuracy in predicting S is over a threshold, say 90%, and not updating the generator if the accuracy is below a threshold, say 60%. We find that this sometimes improves results, but more investigation is needed.

4.5 ADVERSARIAL LEARNED FAIR REPRESENTATIONS (ALFR)

We apply the general setup described in Section 4 to the case of learning fair classifiers as described in Section 3. In this case the sensitive variable S would correspond to some category like gender or race, and the target variable Y would be the attribute we wish to predict using these fair representations.

In this specific case it is worth pointing out that the discrimination y_{disc} of the classifier η is bounded above by the empirical \mathcal{H} -divergence, as shown in Lemma 2 in Appendix A, that is

$$y_{disc} \leq \frac{1}{2} \hat{d}_{\mathcal{H}}(\hat{R}_0, \hat{R}_1), \quad (11)$$

Algorithm 1 Strictly alternating gradient steps.

```

 $\theta, \phi \leftarrow$  initialize network parameters
 $U \leftarrow \text{True}$  ▷ Boolean indicating whether to update parameters  $\theta$  or  $\phi$ .
repeat
   $X, Y, S \leftarrow$  random mini-batch from dataset
   $R \leftarrow \text{Enc}(X)$ 
   $\hat{X} \leftarrow \text{Dec}(R)$ 
   $\hat{Y} \leftarrow \text{Pred}(R)$ 
   $\hat{S} \leftarrow \text{Adv}(R)$ 
   $C \leftarrow \frac{1}{|X|} \sum_{x, \hat{x} \in X, \hat{X}} \|x - \hat{x}\|_2^2$  ▷ Reconstruction loss for the autoencoder.
   $E \leftarrow \frac{1}{|X|} \sum_{y, \hat{y} \in Y, \hat{Y}} y \cdot \log(\hat{y}) + (1 - y) \cdot \log(1 - \hat{y})$  ▷ Log-loss for the predictor.
   $D \leftarrow \frac{1}{|X|} \sum_{s, \hat{s} \in S, \hat{S}} s \cdot \log(\hat{s}) + (1 - s) \cdot \log(1 - \hat{s})$  ▷ Negative log-loss for the adversary.
   $L \leftarrow \alpha C + \beta D + \gamma E$  ▷ Joint loss.
  if  $U$  then ▷ Updating adversary's parameters.
     $\theta \leftarrow \phi + \alpha \nabla_{\phi} L$ 
  else ▷ Updating autoencoder's parameters.
     $\phi \leftarrow \theta - \alpha \nabla_{\theta} L$ 
  end if
   $U \leftarrow \text{not } U$ 
until Deadline

```

where \mathcal{H} is a symmetric hypothesis class on R including η and \hat{R}_0, \hat{R}_1 are the empirical samples given to us. This is because the discrimination between R_0 and R_1 given by the best hypothesis must be at least as good as some particular hypothesis η , assuming $\eta \in \mathcal{H}$. So minimizing the divergence minimizes the discrimination.

4.6 ANONYMIZING IMAGES

We apply the the idea of censoring representations to the application of removing text from images. In this problem the input X is an image and the sensitive variable S describes whether or not the image contains private information (text). Here there is no prediction task and so there is no variable Y . In contrast to ALFR, we are not interested in learning a hidden representation, but the reconstructed image \hat{X} , so in this case we have $R = \hat{X}$. In order to evaluate the model, we need to have a small amount of validation/test data where we have pairs of images with and without the text. This is used to choose hyperparameters, but the model itself never gets to train on example input/output pairs.

5 EXPERIMENTAL RESULTS

We used the *Adam* algorithm with the default parameters for all our optimizations. The experiments were implemented using *theano* (Bergstra et al. (2010), Bastien et al. (2012)) and the python library *lasagne*.

5.1 FAIRNESS

5.1.1 DATASETS

We used two datasets from the UCI repository Lichman (2013) to demonstrate the efficacy of ALFR.

The *Adult* dataset consists of census data and the task is to predict whether a person makes over 50K dollars per year. The sensitive attribute we chose was *Gender*. The data has 45,222 instances and 102 attributes. We used 35 thousand instances for the training set and approximately 5 thousand instances each for the validation and test sets.

The *Diabetes* dataset consists of hospital data from the US and the task is to predict whether a patient will be readmitted to hospital. The sensitive attribute we chose was *Race*, we changed this to a binary variable by creating a new attribute *isCaucasian*. The data has around 100 thousand instances and 235 attributes. We used 80 thousand instances for the training set and approximately 10 thousand instances each for the validation and test sets.

5.1.2 PROTOCOLS AND ARCHITECTURE

To compare ALFR with LFR we split each dataset into training, validation and test sets randomly, we then run 100 experiments per model with different hyperparameters. Then for each value of t considered we selected the model maximizing $y_{t, disc}$ on the validation data. This process was repeated 5 times on different data splits. Since each model sees the same data split, the observations are paired and so we get 5 observations of the difference in performance for each value of t .

In evaluating the results, we want to evaluate the approaches for different possible tradeoffs between accuracy and discrimination, and so we compare with a range of values of $t \in [0, 3]$ and explore hyperparameters using a random search (the 100 settings over hyperparameters are drawn from a product of simple distributions over each hyperparameter). We use random search, as opposed to a sequential, performance driven search, so that we are able to compare the models across a range of values of t . When using these methods in practice one should select the hyperparameters, using Bayesian optimization or a similar approach, to maximize the specific tradeoff one cares about.

We now give details of the priors over hyperparameters used for the random search. The autoencoder in ALFR had $U(\{1, \dots, 3\})$ encoding/decoding layers with $U(\{1, \dots, 100\})$ hidden units, with all hidden layers having the same number of hidden units. Each encoding/decoding unit used the ReLU (Nair & Hinton (2010)) activation. The critic also had $U(\{1, \dots, 3\})$ hidden layers with ReLU activations. The predictor network was simply a logistic regressor on top of the central hidden layer of the autoencoder. In the LFR model the model had $U(\{5, \dots, 50\})$ clusters. In both models the reconstruction error weighting parameter α was fixed at 0.05. For both models we used had $\beta \sim U[0, 50]$ and $\gamma \sim U[0, 10]$.

5.1.3 RESULTS

We found the LFR model was sensitive to hyperparameters/initialization and could often stick during training, but given sufficient experiments we were able to obtain good results. In Figure 1 and Figure 2 we see the results of applying both LFR and ALFR on the *Adult* and *Diabetes* data respectively. In both cases we see that the ALFR model is able to obtain significantly better results across most of the range of possible tradeoffs between accuracy and discrimination. The step changes in these figures correspond to places where the change in tradeoff results in a different form of model. This also clarifies that the results are often not very sensitive to this tradeoff parameter.

We were also interested in the effect of the hyperparameters α , β , γ on the discrimination of the ALFR model. In particular we consider the ratio $\frac{\beta}{\beta + \gamma}$, measuring the relative importance of the dependence term $D(X, R)$ over the prediction error term $E(Y, R)$ in the cost. In Figure 3 we see that the larger β is relative to γ , the lower the discrimination is (up to a point), which matches expectations.

5.2 IMAGE ANONYMIZATION

5.2.1 DATASETS

We used the ‘10k US Adult Faces’ dataset Bainbridge et al. (2013) consisting of 10,168 natural face photographs. We preprocessed the data by rescaling each to 100×80 pixels and converting to grayscale. In addition, for half the training images we added private information, in the form of text overlayed at a random location in the image. We used 200 photographs as a validation set, and 49 for the test set, on both the validation and test sets we have the image both with and without the text for evaluation. In this problem the sensitive variable S indicates whether or not the image contains text.

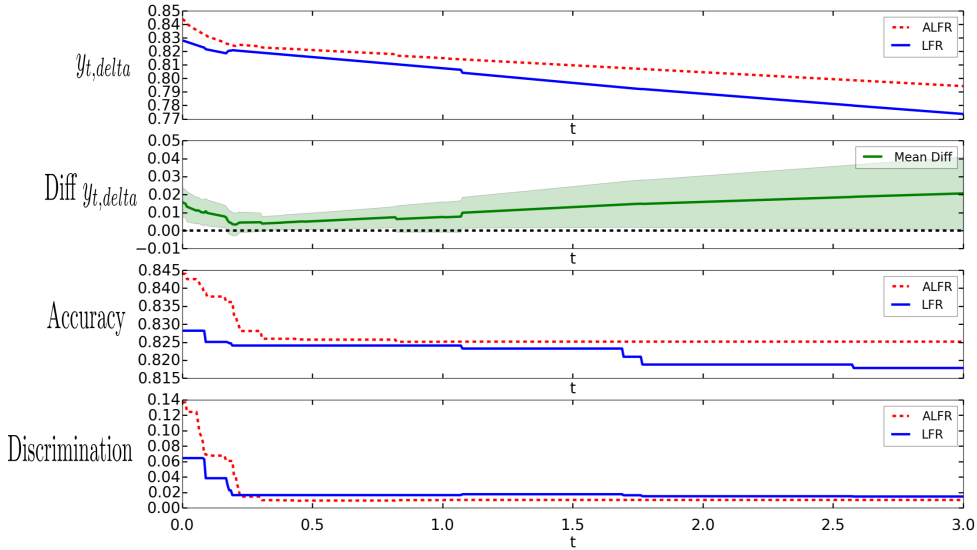


Figure 1: Results on *Adult* dataset. For each value of t the model maximizing $y_{t,delta}$ on the validation set is selected, the plots show the performance of the selected models on the test data. Top row is $y_{t,delta}$. Second row down shows the mean paired difference between the $y_{t,delta}$ for the ALFR model and LFR model, where positive values favour ALFR. We also give a 95% CI around the mean. Third row down is y_{acc} . Bottom row is y_{disc} . We see from the top row that the ALFR model has better $y_{t,delta}$ for every setting of t considered. Moreover the difference is significant for most values of t (that is, the CI does not include zero).

5.2.2 PROTOCOLS AND ARCHITECTURE

The global image autoencoder model we used was an expert patch based model, using 5×5 patches. The expert model consists of two parts, a patch classifier and a neural patch autoencoder. The image reconstruction is formed by simply copying the patch if the patch classifier predicts there to be no text-label in the patch. Otherwise it uses the patch autoencoder to construct the patch. The patch classifier is pretrained with weak-supervision using image level labels for each patch. The decision boundary for the patch adversary is a hyperparameter, optimized to use the autoencoder if the probability of a text-label is > 0.7 in this setting. Altogether the whole image was reconstructed from the input image using the expert patch based model for each patch of the image.

Along with the image autoencoder is the full image adversary, which takes the whole reconstructed image and classifies whether the image has a text-label present or not.

The patch classifier had a single hidden layer with 200 ReLU units. The autoencoder also had a single hidden layer with 2000 ReLU units. The adversary had two convolutional layers each with 10 filters of size 3×3 interspersed with two max-pooling layers with pooling size 4, this was followed by a dense layer with 1000 hidden units with ReLU activations. Other hyperparameters were the α and β weights, which were chosen to be $\alpha = 1$ and $\beta = 10$.

All hyperparameters were chosen by evaluation on the validation data. The validation data consists of input/output pairs (x_{in}, x_{out}) where x_{in} contains text, and x_{out} is the corresponding image without text. The performance was measured using the mean-square error between the autoencoder’s output \hat{x} given x_{in} and the target x_{out} .

5.2.3 RESULTS

Sample images produced by the trained model on the test data are shown in Figure 4. The model learns to imagine what the image would have looked like had there been no text, despite having

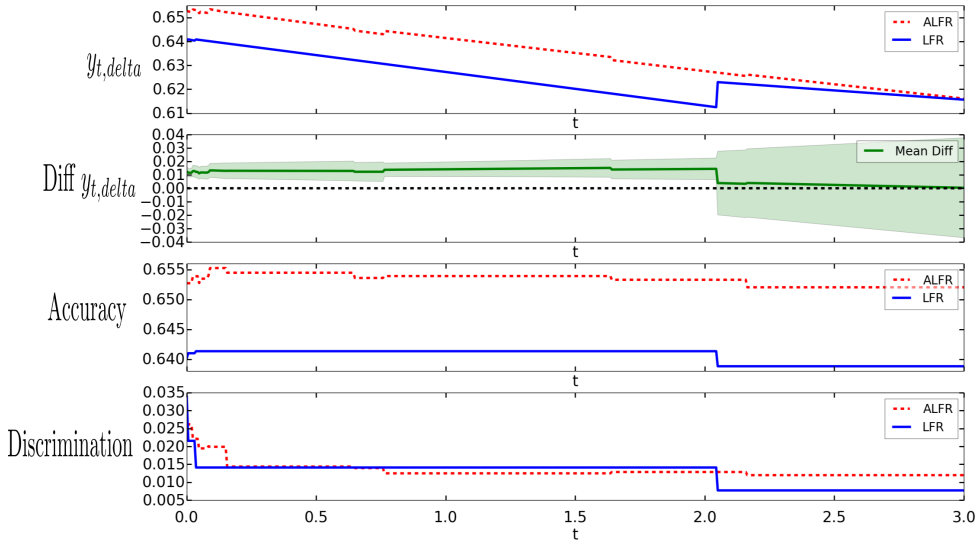


Figure 2: Results on *Diabetes* dataset. For each value of t the model maximizing $y_{t,delta}$ on the validation set is selected, the plots show the performance of the selected models on the test data. Top row is $y_{t,delta}$. Second row down shows the mean paired difference between the $y_{t,delta}$ for the ALFR model and LFR model, where positive values favour ALFR. We also give a 95% CI around the mean. Third row down is y_{acc} . Bottom row is y_{disc} . We see from the top row that the ALFR model has better $y_{t,delta}$ for every setting of t considered. We also see that the difference is significant for $\approx t \leq 2$ (that is, the CI does not include zero).

never been given example input/output pairs. The produced images are quite plausible, but artifacts become apparent when zooming in. We believe that the quality of the images could be substantially improved through the use of a convolutional autoencoder on a larger dataset, since this could take into account a wider context than a patch when removing the text.

In this application the flexibility of the adversarial framework as compared with a clustering approach becomes apparent, it would be extremely difficult to get an LFR-style approach to work for images, since it must reconstruct images as a convex combination of template images.

6 CONCLUSIONS AND FUTURE WORK

We have shown how the adversarial approach can be adapted to the task of removing sensitive information from representations. Our model ALFR improves upon a related approach whilst at the same time being more flexible. We demonstrate this flexibility by showing how the same setup can be used to remove text from an image, with encouraging results.

As has been noted before it is difficult to train adversarial models owing to the unstable dynamic between actor and adversary. There is work to be done in the future in developing theory, or at least heuristics, for improving the stability of the training process.

Following up from the application on images we would like to investigate the more challenging problem of removing more pervasive information from an image, for instance removing gender from a face.

Another interesting problem to investigate would be obscuring text in images where we only have negative examples of images with text. With no further assumptions our method would not be applicable, but if we assume that we have some information about the text then we can gain some traction. For example if the text is the name of the person in the image, and we know the name of the

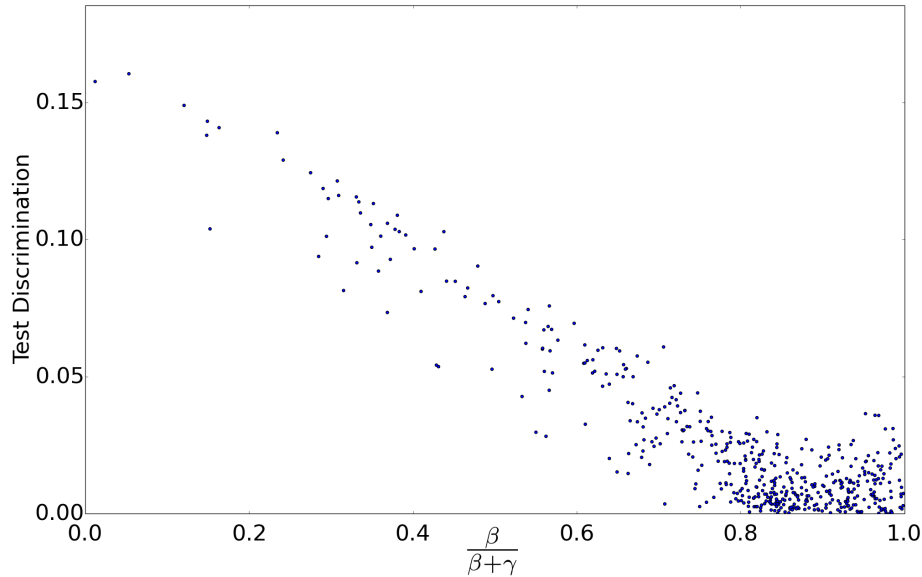


Figure 3: A scatter plot of $\frac{\beta}{\beta+\gamma}$ versus the test discrimination of the ALFR model on the *Adult* dataset. We see an approximately linear relation up to a certain point, after which further relative increase in β has little effect on the discrimination.

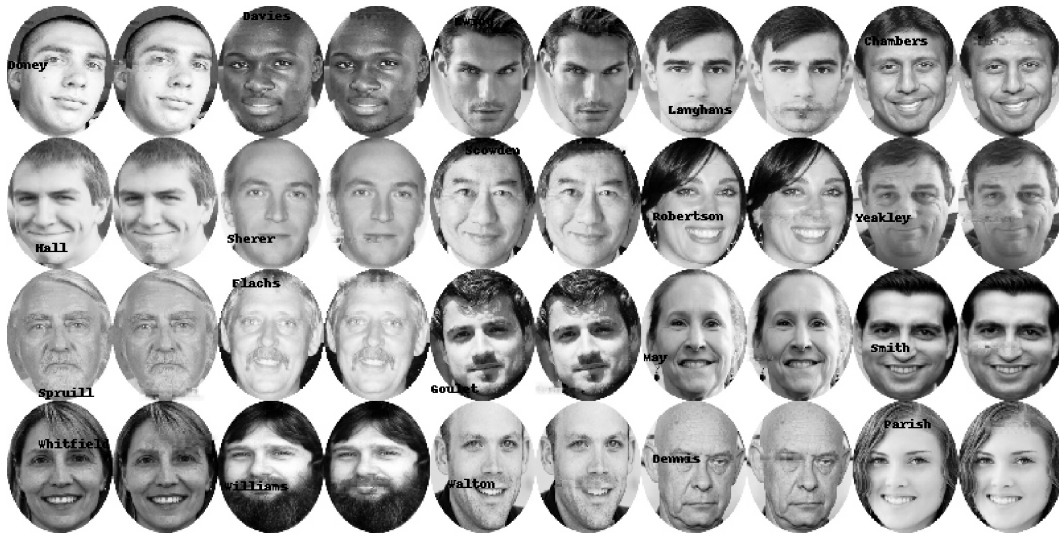


Figure 4: Image anonymization results on the test set. In each pair of faces the left image is the input to the autoencoder, and the right image is the censored output.

person in the image, then the adversary could be trained to predict a bag-of-characters of the name, whereas the autoencoder would be trained to make this task difficult for the adversary. The result should be a blurring, rather than removal of the text. One issue one would face in this approach would be a lack of any ground-truth examples for validation, since there are many ways to obscure text.

ACKNOWLEDGMENTS

This work was supported in part by the EPSRC Centre for Doctoral Training in Data Science, funded by the UK Engineering and Physical Sciences Research Council (grant EP/L016427/1) and the University of Edinburgh.

REFERENCES

- Bainbridge, Wilma A, Isola, Phillip, and Oliva, Aude. The intrinsic memorability of face photographs. *Journal of Experimental Psychology: General*, 142(4):1323, 2013.
- Bastien, Frédéric, Lamblin, Pascal, Pascanu, Razvan, Bergstra, James, Goodfellow, Ian J., Bergeron, Arnaud, Bouchard, Nicolas, and Bengio, Yoshua. Theano: New features and speed improvements. Deep Learning and Unsupervised Feature Learning NIPS 2012 Workshop, 2012.
- Ben-David, Shai, Blitzer, John, Crammer, Koby, Pereira, Fernando, et al. Analysis of representations for domain adaptation. *Advances in neural information processing systems*, 19:137, 2007.
- Ben-David, Shai, Blitzer, John, Crammer, Koby, Kulesza, Alex, Pereira, Fernando, and Vaughan, Jennifer Wortman. A theory of learning from different domains. *Machine Learning*, 79(1-2):151–175, 2010. ISSN 0885-6125. doi: 10.1007/s10994-009-5152-4. URL <http://dx.doi.org/10.1007/s10994-009-5152-4>.
- Bergstra, James, Breuleux, Olivier, Bastien, Frédéric, Lamblin, Pascal, Pascanu, Razvan, Desjardins, Guillaume, Turian, Joseph, Warde-Farley, David, and Bengio, Yoshua. Theano: A CPU and GPU math expression compiler. In *Proceedings of the Python for Scientific Computing Conference (SciPy)*, June 2010. Oral Presentation.
- Calders, Toon and Verwer, Sicco. Three Naive Bayes approaches for discrimination-free classification. *Data Mining and Knowledge Discovery*, 21(2):277–292, 2010. ISSN 1384-5810. doi: 10.1007/s10618-010-0190-x. URL <http://dx.doi.org/10.1007/s10618-010-0190-x>.
- Denton, Emily, Chintala, Soumith, Szlam, Arthur, and Fergus, Rob. Deep generative image models using a Laplacian Pyramid of adversarial networks. *arXiv preprint arXiv:1506.05751*, 2015.
- Erickson, Zackory, Compiano, Jared, and Shin, Richard. Neural networks for improving wearable device security.
- Ganin, Yaroslav, Ustinova, Evgeniya, Ajakan, Hana, Germain, Pascal, Larochelle, Hugo, Laviolette, François, Marchand, Mario, and Lempitsky, Victor S. Domain-adversarial training of neural networks. *CoRR*, abs/1505.07818, 2015. URL <http://arxiv.org/abs/1505.07818>.
- Gauthier, J. Conditional generative adversarial nets for convolutional face generation, 2015.
- Goodfellow, Ian J. On distinguishability criteria for estimating generative models. *arXiv preprint arXiv:1412.6515*, 2014.
- Goodfellow, Ian J., Pouget-Abadie, Jean, Mirza, Mehdi, Xu, Bing, Warde-Farley, David, Ozair, Sherjil, Courville, Aaron C., and Bengio, Yoshua. Generative adversarial nets. In *Advances in Neural Information Processing Systems 27: Annual Conference on Neural Information Processing Systems 2014, December 8-13 2014, Montreal, Quebec, Canada*, pp. 2672–2680, 2014. URL <http://papers.nips.cc/paper/5423-generative-adversarial-nets>.
- Kamiran, Faisal and Calders, Toon. Classification with no discrimination by preferential sampling. In *2nd International Conference on Computer, Control and Communication*, pp. 1–6, 2009.
- Kamishima, T., Akaho, S., and Sakuma, J. Fairness-aware learning through regularization approach. In *Data Mining Workshops (ICDMW), 2011 IEEE 11th International Conference on*, pp. 643–650, Dec 2011. doi: 10.1109/ICDMW.2011.83.

- Kifer, Daniel, Ben-David, Shai, and Gehrke, Johannes. Detecting change in data streams. In *Proceedings of the Thirtieth International Conference on Very Large Data Bases - Volume 30, VLDB '04*, pp. 180–191. VLDB Endowment, 2004. ISBN 0-12-088469-0. URL <http://dl.acm.org/citation.cfm?id=1316689.1316707>.
- Kingma, Diederik and Ba, Jimmy. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.
- Korayem, Mohammed, Templeman, Robert, Chen, Dennis, Crandall, David J., and Kapadia, Apu. ScreenAvoider: protecting computer screens from ubiquitous cameras. *CoRR*, abs/1412.0008, 2014. URL <http://arxiv.org/abs/1412.0008>.
- Lichman, M. UCI machine learning repository, 2013. URL <http://archive.ics.uci.edu/ml>.
- Louizos, C., Swersky, K., Li, Y., Welling, M., and Zemel, R. The variational fair auto encoder. *ArXiv e-prints*, November 2015.
- Nair, Vinod and Hinton, Geoffrey E. Rectified linear units improve restricted boltzmann machines. In *Proceedings of the 27th International Conference on Machine Learning (ICML-10), June 21-24, 2010, Haifa, Israel*, pp. 807–814, 2010. URL <http://www.icml2010.org/papers/432.pdf>.
- Rudy, Jan and Taylor, Graham. Generative class-conditional autoencoders. *arXiv preprint arXiv:1412.7009*, 2014.
- Schmidhuber, J. Learning factorial codes by predictability minimization. Technical Report CU-CS-565-91, Dept. of Comp. Sci., University of Colorado at Boulder, December 1991.
- Schmidhuber, J, Eldracher, M, and Foltin, B. Semilinear predictability minimization produces well-known feature detectors. *Neural Computation*, 8(4):773–786, May 1996. ISSN 0899-7667. doi: 10.1162/neco.1996.8.4.773.
- Schraudolph, Nicol N., Eldracher, Martin, and Schmidhuber, Jürgen. Processing images by semi-linear predictability minimization. *Network: Computation in Neural Systems*, 10(2):133–169, 1999.
- Zafar, Muhammad Bilal, Valera, Isabel, Gomez-Rodriguez, Manuel, and Gummadi, Krishna P. Fairness constraints: A mechanism for fair classification. *CoRR*, abs/1507.05259, 2015. URL <http://arxiv.org/abs/1507.05259>.
- Zemel, Rich, Wu, Yu, Swersky, Kevin, Pitassi, Toni, and Dwork, Cynthia. Learning fair representations. In Dasgupta, Sanjoy and Mcallester, David (eds.), *Proceedings of the 30th International Conference on Machine Learning (ICML-13)*, volume 28, pp. 325–333. JMLR Workshop and Conference Proceedings, May 2013. URL <http://jmlr.org/proceedings/papers/v28/zemel13.pdf>.

A THE \mathcal{H} -DIVERGENCE

In this appendix we describe the notion of a \mathcal{H} -divergence, as developed in Kifer et al. (2004) and Ben-David et al. (2007). The \mathcal{H} -divergence is a way of measuring the difference between two distributions using classifiers.

Definition 1. A *hypothesis* for a random variable X is a mapping $\eta : \mathcal{X} \rightarrow \{0, 1\}$.

Definition 2. A *hypothesis class* \mathcal{H} for a random variable X is a collection of hypotheses on X .

Definition 3. A *symmetrical hypothesis class* \mathcal{H} is a hypothesis class such that for each $\eta \in \mathcal{H}$, the inverse hypothesis $\bar{\eta}$ defined $\bar{\eta}(x) = 1 - \eta(x)$ is also in \mathcal{H} .

Now we can define the divergence.

Definition 4. Given two random variables X_0, X_1 on a common space \mathcal{X} and a hypothesis class \mathcal{H} on \mathcal{X} , the \mathcal{H} -divergence between X_0 and X_1 is

$$d_{\mathcal{H}}(X_0, X_1) = \sup_{\eta \in \mathcal{H}} 2 |\mathbb{E} \eta(X_0) - \mathbb{E} \eta(X_1)|.$$

In case \mathcal{H} is symmetric, Ben-David et al. (2010) show that $d_{\mathcal{H}}(X_0, X_1)$ can be approximated empirically.

Definition 5. Let \mathcal{H} be a symmetrical hypothesis class on random variables X_0, X_1 on a common space \mathcal{X} . Now given i.i.d samples $A = \{a_1, \dots, a_n\}$ from X_0 and i.i.d samples $B = \{b_1, \dots, b_m\}$ from X_1 , we define the *empirical \mathcal{H} -divergence* between X_0, X_1 to be

$$\hat{d}_{\mathcal{H}}(X_0, X_1) = \sup_{\eta \in \mathcal{H}} 2 \left[\frac{1}{n} \sum_{x \in A} \eta(x) - \frac{1}{m} \sum_{x \in B} \eta(x) \right],$$

The nature of this empirical approximation is shown in the following probabilistic bound from Ben-David et al. (2010).

Lemma 1. Let \mathcal{H} be a symmetrical hypothesis class with VC dimension d on random variables X_0, X_1 on a common space \mathcal{X} . Now given i.i.d samples $A = \{a_1, \dots, a_n\}$ from X_0 and i.i.d samples $B = \{b_1, \dots, b_m\}$ from X_1 , we have that, for any $\delta \in (0, 1)$, with probability at least $1 - \delta$,

$$d_{\mathcal{H}}(X_0, X_1) \leq \hat{d}_{\mathcal{H}}(A, B) + \sqrt{\frac{d \log(2m) + \log(\frac{2}{\delta})}{m}}.$$

So we can see that minimizing the capability of an adversary to tell the difference between two distributions relates to minimizing an \mathcal{H} -divergence. The empirical divergence can be straightforwardly related to the discrimination of a classifier.

Lemma 2. Let X, S, Y and R be as described in Section 4. Let $\eta : \mathcal{R} \rightarrow \mathcal{Y}$ be our classifier and y_{disc} the discrimination as described in Section 3. Then

$$y_{disc} \leq \frac{1}{2} \hat{d}_{\mathcal{H}}(\hat{R}_0, \hat{R}_1),$$

where \mathcal{H} is a symmetric hypothesis class on R including η and \hat{R}_0, \hat{R}_1 are the representations of the empirical samples.

Proof. Recall that

$$y_{disc} = \left| \frac{\sum_{r \in \hat{R}_0} \eta(r)}{|\hat{R}_0|} - \frac{\sum_{r \in \hat{R}_1} \eta(r)}{|\hat{R}_1|} \right|,$$

where $m = |\hat{R}_0| = |\hat{R}_1|$. We simply observe that

$$\begin{aligned}
 \left| \frac{\sum_{r \in \hat{R}_0} \eta(r)}{|\hat{R}_0|} - \frac{\sum_{r \in \hat{R}_1} \eta(r)}{|\hat{R}_1|} \right| &\leq \sup_{\eta^* \in \mathcal{H}} \left| \frac{\sum_{r \in \hat{R}_0} \eta^*(r)}{|\hat{R}_0|} - \frac{\sum_{r \in \hat{R}_1} \eta^*(r)}{|\hat{R}_1|} \right| \\
 &= \sup_{\eta^* \in \mathcal{H}} \left[\frac{\sum_{r \in \hat{R}_0} \eta^*(r)}{|\hat{R}_0|} - \frac{\sum_{r \in \hat{R}_1} \eta^*(r)}{|\hat{R}_1|} \right] \\
 &= \frac{1}{2} \hat{D}_{\mathcal{H}}(\hat{R}_0, \hat{R}_1)
 \end{aligned}$$

where for the inequality we use the fact that $\eta \in \mathcal{H}$ and for the first equality we use the fact that \mathcal{H} is a symmetric hypothesis class.

□